Listing of claims:

1. (Currently amended) A computer-readable medium having computer-executable instructions for protecting network domain data against unauthorized modification in a distributed computer network having a plurality of network domains, comprising:

receiving, at a first computing machine, a request to modify an object associated with a shared data structure, wherein the shared data structure is shared by the plurality of network domains ~~spanning a plurality of domains~~, wherein the first computing machine resides in at least one of the network domains ~~a domain~~, wherein the object includes ~~including~~ a security descriptor identifying an owner network domain of the object ~~in the plurality of domains~~ and ~~having~~ an identification of one or more users;

determining whether the first computing machine resides in ~~is within~~ the owner network domain by retrieving from the security descriptor the identity of the owner network domain and comparing the owner network domain identity to the network domain within which the first computing machine resides; and

~~if the first computing machine is not within the owner domain,~~ rejecting the request to modify the object when the first computing machine does not reside in the owner network domain.

2. (Currently amended) The computer-readable medium of claim 1, further comprising, ~~if the first computing machine is within the owner domain,~~ allowing the request to modify the object when the first computing machine resides in the owner network domain.

3. (Currently amended) The computer-readable medium of claim 1, wherein the shared data structure includes at least one data store that is replicated among each of the plurality of network domains, and wherein the object is contained within the replicated data store.

4. (cancelled)

5. (Currently amended) The computer-readable medium of claim 1, wherein the security descriptor further comprises a field that indicates whether a special security evaluation should be performed on requests to modify the object, and wherein the computer-executable instructions further comprise, ~~if the field indicates that the special security evaluation should be performed,~~ causing the special security evaluation to be performed when the field indicates that the special security evaluation should be performed.

6. (Currently amended) The computer-readable medium of claim 5, wherein the special security evaluation comprises ~~causing~~ requesting that a second computing machine within the owner network domain evaluate whether an entity issuing the request to modify the object is authorized to modify the object.

7. (Currently amended) A computer-implemented method for protecting network domain data against unauthorized modification in a distributed computer network having a plurality of network domains, comprising:

receiving, from a requester at a first machine in a first network domain in ~~a~~ the plurality of network domains, a request to modify an object, the request including a security token identifying at least one group of which the requester is a member, the object having an associated security descriptor identifying an owner network domain ~~for~~ of the object and having an identification of one or more users, the object having a flag to identify whether a special security evaluation is to be performed on requests to modify the object;

determining from the flag whether the special security evaluation is to be performed on the request to modify the object;

~~if the flag indicates in the affirmative, then~~ performing the special security evaluation on the request to modify the object when the flag indicates in the affirmative, wherein the special security evaluation on the request to modify the object is performed by passing the security token associated with the request and the security descriptor associated with the object to the owner network domain for evaluation; and

~~if the special security evaluation approves the request to modify the object then~~ allowing the request to modify the object to proceed when the special security evaluation approves the request to modify the object.

8. (cancelled)

9. (Currently amended) The computer-readable medium of claim 7, further comprising, ~~if the flag indicates in the negative, then~~ performing a security evaluation on the request to modify the object when the flag indicates in the negative.

10. (original) The computer-readable medium of claim 9, wherein the security evaluation comprises comparing the security token with the security descriptor to determine whether the requester is a member of any groups that have been granted permission to access the object.

11. (original) The computer-readable medium of claim 10, wherein the security evaluation further comprises determining whether the request to modify the object is a modification for which the requester is privileged on the first machine regardless of whether the requester is a member of any groups that have been granted permission to access the object.

12. (Currently amended) The computer-readable medium of claim 11, wherein the security evaluation further comprises denying the request when the requester is privileged to perform the request to modify the object, the requested modification is a fundamental modification of the object, and the first network domain is not the owner network domain of the object. ~~if the requester is privileged to perform the request to modify the object, and the requested modification is a fundamental modification of the object, then denying the request if the first domain is not the owner domain for the object~~.

13. (Currently amended) A computer-readable medium having computer-executable components to protect network domain data against unauthorized modification in a distributed computer network having a plurality of network domains; comprising:

a shared data structure of the ~~that spans a~~ plurality of domains, at least two network domains in the plurality of network domains having a transitive trust relationship wherein a user authentication within one of the two network domains is honored in the other of the two network domains, the shared data structure having at least one data store that is replicated among each of the plurality of network domains;

an object stored within the data store, the object having a plurality of attributes, at least one of the attributes being related to security access rights associated with the object, the security access rights including an owner network domain identifier identifying one of the domains within the plurality of domains, and ~~having~~ an identification of one or more users; and

a security system configured to receive a request to modify the object, to retrieve from the object the owner network domain identifier, to compare the owner network domain identifier with an identifier of a network domain from which the request originated, and to reject the request to modify the object if the owner network domain identifier does not match the identifier of the network domain from which the request originated.

14. (Currently amended) The computer-readable medium of claim 13, wherein:

the security access rights associated with the object further comprise an indicator that an attempt to access the object is to be evaluated within the network domain identified by the owner network domain; and

the security system is further configured to, prior to performing a security evaluation on a received request to modify the object, determine from the indicator whether the request to modify the object should be evaluated within the network domain identified by the owner network domain, and if so, to return a notification to the requestor that the security evaluation is to be evaluated within the network domain identified by the owner network domain.

15. (Currently amended) The computer-readable medium of claim 14, wherein the notification to the requestor comprises a referral message including an identification of the owner network domain.

16. (Currently amended) The computer-readable medium of claim 13, wherein the security system is further configured to determine whether the request to modify the object originated within a particular network domain of the plurality of network domains, and if so, ~~then to~~ perform a standard security evaluation of the request to modify the object without resort to the owner network domain.

17. (Currently amended) The computer-readable medium of claim 16, wherein the particular network domain is a root network domain of the shared data structure.

18. (original) The computer-readable medium of claim 13, wherein the shared data structure comprises a directory service and wherein the at least one data store comprises configuration data associated with the directory service.

19. (original) The computer-readable medium of claim 13, wherein the shared data structure comprises a directory service and wherein the at least one data store comprises schema data associated with the directory service.

20. (Currently amended) The computer-readable medium of claim 13, wherein the at least one attribute comprises a security descriptor and permissions associated with the one or more users, and the owner network domain identifier is part of an owner security identifier.

21. (previously presented) The computer-readable medium of claim 1, wherein the security descriptor includes permissions associated with the one or more users.

22. (previously presented) The computer-readable medium of claim 7, wherein the security descriptor includes permissions associated with the one or more users.